International Journal of Innovative
Computing, Information and Control
Volume **5**, Number **10(A)**, October **2009**

ICIC International ©2009 ISSN 1349-4198
pp. **3059–3069**

MODULAR SQUARE-AND-MULTIPLY OPERATION FOR QUADRATIC RESIDUE BASES

Chin-Chen Chang[1] and Yeu-Pong Lai[2]

[1]Department of Information Engineering and Computer Science
Feng Chia University
Taichung, 40724, Taiwan
ccc@cs.ccu.edu.tw

[2]Department of Computer Science and Information Engineering
Chung Cheng Institute of Technology
National Defense University
Tauyuan, 33509, Taiwan
lai@ccit.edu.tw

Received May 2008; revised October 2008

Abstract. *This paper introduces a new operation for modular exponentiation operations. The number of modular operations will determine the computing performance of modular exponentiation under the assumption that the complexity of modular multiplication is the same as that of modular square. Unlike other schemes that are devoted to the reduction of the number of modular multiplication operations, the proposed operation performs modular square operation and modular multiplication operation together. To accelerate the proposed modular square-and-multiply operation, the lookup table scheme is introduced. The elements in this lookup table are computed according to the Chinese Remainder Theorem after the modulus is given. Every element is a partial result of modular square operations. The modular square operation can then work very efficiently. The modular square-and-multiply operation is derived from the modular square operation with a quadratic residue base. To sum up, modular exponentiation operations processed by the proposed operation can not only get speeded up in reducing the number of modular operations but also improve the performance of every modular operation.*
Keywords: Chinese Remainder Theorem, Quadratic residue, Modular exponentiation, Lookup table, Modular square, Modular multiplication, Computer arithmetic

1. **Introduction.** Modular operations always play an important role in computer arithmetic for their characteristic of confining the operand scalar within certain bit lengths. The computing performance is therefore speeded up. Besides, the computing overflow problem is also eliminated. As known, the data transmitted and stored within computers are always in fixed bit lengths due to the limited bandwidth of data bus. Another reason for modular operations to be so important is that they are massively used in cryptosystems. In cryptosystems, such as those cryptosystems based on the RSA scheme or the ElGamal scheme, the modular exponentiation operations are performed for encrypting and decrypting secret message, [3][8]. As a result, the efficiency of the operations is the focus of research. So far, there have been many accelerating techniques dedicated to the enhancement of the efficiency, both in hardware and software designs [4].

The modular exponentiation operation computes $B^x \ mod \ N$, where the variables B, x and N refer respectively to the base number, the exponent and the modulus. Each modular exponentiation consists of two "separated" parts, the modular multiplication and the modular square. Because these modular square operations are compulsory, the number